2.11 Polynômes irréductibles sur $\mathbb{F}_q$

Référence : S. Francinou, H. Gianella, *Exercices de mathématiques pour l'agrégation, Algèbre 1*, Masson, 1997.

Leçons concernées : 123, 125, 141, 190.

Soit p un nombre premier et q une puissance de p.

Théorème 1. *On note $\mathcal{P}_q(n)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$ et $I(q,n)$ son cardinal. Alors*

$$I(q,n) = \frac{1}{n}\sum_{d|n}\mu\Big(\frac{n}{d}\Big)q^d$$

et donc $I(q,n) \underset{n\to\infty}{\sim} \dfrac{q^n}{n}$.

Démonstration. On commence par montrer que

$$X^{q^n} - X = \prod_{d|n}\prod_{P\in\mathcal{P}_q(d)} P(X).$$

En effet, si $d \mid n$ et si $P \in \mathcal{P}_q(d)$, on considère $K = \mathbb{F}_q[X]/(P)$ qui est un corps de cardinal q^d, et donc, pour $x \in K$, $x^{q^d} = x$. Or, on a,

$$x^{q^n} = \underbrace{\big(\cdots\big(x^{q^d}\big)^{q^d}\cdots\big)^{q^d}}_{n/d \text{ fois}}$$

et donc pour $x \in K$, $x^{q^n} = x$, en particulier, $\overline{X}^{q^n} = \overline{X}$ et donc $\overline{X}^{q^n} - \overline{X} = 0$ dans $\mathbb{F}_q[X]/(P)$, c'est-à-dire que $P \mid X^{q^n} - X$. Par le lemme de Gauss, on déduit que $\prod_{d|n}\prod_{P\in\mathcal{P}_q(d)} P(X) \mid X^{q^n} - X$.

Réciproquement, soit P un diviseur irréductible de $X^{q^n} - X$ de degré d. Puisque $\mathbb{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$, P est scindé sur $\mathbb{F}_{q^n}$. Soit alors $x \in \mathbb{F}_{q^n}$ une racine de P. On a d'après le théorème de la base télescopique

$$n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(x)][\mathbb{F}_q(x) : \mathbb{F}_q].$$

Or P est irréductible sur $\mathbb{F}_q$ donc $[\mathbb{F}_q(x) : \mathbb{F}_q] = d$, ainsi, $d \mid n$.

Enfin, $X^{q^n} - X$ n'a pas de facteurs multiples, en effet si c'était le cas il serait à racines multiples dans $\mathbb{F}_{q^n}$ son corps de décomposition sur $\mathbb{F}_q$. Or $(X^{q^n} - X)' = -1$ dans $\mathbb{F}_{q^n}$ (car $\mathrm{car}(\mathbb{F}_{q^n}) = p$) et donc $X^{q^n} - X$ est à racines simples sur $\mathbb{F}_{q^n}$.

On montre maintenant la proposition suivante :

Proposition 2. *Soit $f : \mathbb{N}^* \to \mathbb{C}$ et μ la fonction de Möbius. Si pour $n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} f(d)$, alors pour $n \in \mathbb{N}^*$, $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.*

Démonstration. On remarque d'abord que ($d \mid n$ et $d' \mid \frac{n}{d}$) si et seulement si $dd' \mid n$. Ainsi, on a

$$\sum_{d|n} \mu(d) g\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \sum_{d' | \frac{n}{d}} f(d') = \sum_{dd'|n} \mu(d) f(d') = \sum_{d'|n} f(d') \sum_{d | \frac{n}{d'}} \mu(d).$$

Or on sait que si $m \neq 1$, $\sum_{d|m} \mu(d) = 0$[1], d'où le résultat. □

On a, en prenant les degrés dans la factorisation de $X^{q^n} - X$,

$$q^n = \sum_{d|n} d \cdot I(q, d).$$

Ainsi, en appliquant la formule d'inversion de Möbius avec $g(d) = q^d$ et $f(d) = d \cdot I(q, d)$, on obtient

$$I(q, n) = \frac{1}{n} \sum_{d|n} \mu\Big(\frac{n}{d}\Big) q^d.$$

On note alors $r_n = \sum_{d|n,\ d<n} \mu(\frac{n}{d}) q^d$. On a,

$$|r_n| \leqslant \sum_{d|n,\ d<n} q^d \leqslant \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q^d = \frac{q^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{q - 1}$$

et donc $r_n \underset{+\infty}{=} o(q^n)$. Or $I(q, n) = \dfrac{q^n + r_n}{n}$, et donc $I(q, n) \underset{n \to \infty}{\sim} \dfrac{q^n}{n}$. □

1. Si $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\sum_{d|m} \mu(d) = \sum_{\beta \leqslant \alpha} \mu(p_1^{\beta_1} \cdots p_r^{\beta_r}) = \sum_{\beta \in \{0,1\}^r} (-1)^{|\beta|} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = 0$